REMARKS

Claims 1-18 are pending in the application. Claims 1, 5-7, and 11-12 have been amended herein. Claims 2-4, 9-10 and 13-18 have been canceled. Favorable reconsideration of the application, as amended, is respectfully requested.

I. REJECTION OF CLAIMS UNDER 35 USC § 103

Claims 1, 5-8, and 11-12 stand rejected under 35 USC 103 as being unpatentable over US Patent 6,327,578 to Linehan in view of US Patent 6,061,449 to Canedlore et al.

General Discuss of Linehan

Linehan teaches a system for credit card processing where a merchant obtains an authorization token approving a credit card transaction from a credit card issuing system through the consumer's system (called a wallet) as shown in Figure 2a or directly from the issuer system as shown in Figure 4 (C8, L16-L19). The merchant passes the authorization token to the merchant's bank over the Internet and payment against the authorization is requested by the merchant's bank over a private network. (See generally Figure 2a)

To assure that the authorization from the credit card issuer is valid, the following process shown in Figure 3 used:

1. The merchant sends a wallet initiation message to the consumer. The wallet initiation message includes the payment amount and is digitally signed by the Merchant (Figure 3, Step 304).

2. The Consumer authenticates himself or herself to the wallet software using a User ID/Password combination (Figure 3, step 306).

3. The wallet software sends the initiation message to a gateway system of the credit card issuer (Figure 3, step 306).

4. The Issuer verifies the merchant's digital signature (Figure 3, step 308)

5. If authorized, the Issuer sends a signed authorization token along with the Issuer's certificate. The signed authorization token comprises the initiation message and a reference to the consumer's credit card (Figure 3, step 310).

6. The consumer passes the authorization token to the merchant.

In a variation, the authorization token may be passed directly to the merchant (Figure 4 and C8, L16-L19).

In another variation a smart card is used to authenticate the consumer. Prior to generating the authorization token, the Issuer can verify that the consumer's smart card is present by passing a challenge message to the consumer computer which passes the challenge to the smart card reader which passes the challenge to the smart card. The smart card signs the challenge with its digital signature and returns the signed challenge response. The issuer verifies the smart card's signature to verify the consumer's identity. (Figure 2C and C7, L21-L38).

It must be appreciated that in all of the systems disclosed by Lineham, the authorization token is generated by passing the transaction (or an indication of the transaction) to the issuer gateway and then the authorization token is generated by the issuer gateway. The processed used by the issuer for generating the authorization token is shown in Figure 8. This is distinct from applicant's invention wherein the authorization message is generated by the remote system using a unique multi-step process wherein it can be generated without a need to transfer the electronic fund transfer disbursement file to the remote system.

General Discussion of Candelore et al.

The teachings of Candelore et al. relate to storing program information on a disk (or other storage) in an encrypted manner to avoid pirating.

In on embodiment, not only is chain block encryption used, but the blocks are read from the storage device in a random sequence and dummy data blocks may be communicated between the storage and the secure circuit to further obfuscate the program information.

Note, it must be appreciated that while Candelore et al. suggest the creation of dummy data, it does not teach or suggest the applicant's unique use of dummy data. In the context of Candelore et al. is for purposes of intermixing dummy data blocks with encrypted data blocks to further obscure the data.

This is entirely different than a step of the applicants invention wherein: i) dummy data is used as input to a file authentication component to obtain a dummy authorization message (e.g. an authorization message with the correct data structure by including dummy data within its data fields); and ii) a real authorization message is created from the dummy authorization message by substituting real data in place of the dummy data within certain data fields.

Independent Claim 1

The applicant's invention, as set forth in amended claim 1, Relates to a method for operating a server to generate an electronic funds submission for transfer to a payments processor. The electronic funds submission comprises an electronic funds transfer disbursement file and an authorization message of a predetermined data structure. The authorization message is received from a remote client system. The method comprises:

A. generating a digest of the electronic fund transfer disbursement file by performing a hash on the electronic fund transfer disbursement file.

B. transferring the digest to the remote system.

C. transferring authorization control code to the remote system. The authorization control is executed by the remote system to generate the authorization message on the remote system and return the authorization message to the server. Generating the authorization message comprising the following steps:

i) generating additional message attributes;

ii) generating authenticated attributes, the authenticated attributes comprising the additional message attributes and the digest;

iii) generating a digital signature of the authenticated attributes by

passing the authenticated attributes to a file authentication component of the remote system as part of a digital signature request;

iv) generating a dummy data string;

v) generating a dummy authorization message with the predetermined data structure by passing the dummy data string to the file authentication component of the remote system as part of an authorization response request. The dummy authorization message includes:

a) a digest of the dummy data string;

b) a digital signature of the digest of the dummy data string,

c) a digital certificate corresponding to the digital signature;

vi) generating the authorization message from the dummy authorization message by making the following replacements within the dummy authorization message:

a) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and

b) replacing the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer disbursement file;

D. the server further receiving the authorization message from the remote system;

E. combining the electronic fund transfer disbursement file with the authorization message to create the electronic funds submission; and

F. transferring the electronic funds submission to the payments processor.

Of the claimed steps of the applicants invention, at least steps v) and vi) are not taught or suggested by Linehan, Candelore et al., nor the other art of record. Further, neither Linehan, Candelore et al. nor the other art of record suggest inclusion of such steps nor describe a system where inclusion of the applicant's unique steps would be beneficial.

Independent Claim 7

Claim 7, as amended, also relates to a method for operating a server to generate an electronic fund transfer submission for transfer to a payments processor. Like claim 1, the electronic fund transfer submission comprises an electronic funds transfer disbursement file and an authorization message of a predetermined data structure. The authorization message is received from a remote client system. The method comprises:

A. generating a digest of the electronic fund transfer disbursement file by performing a hash on the electronic fund transfer disbursement file.

B. transferring the digest to the remote system.

C. receiving the authorization message from the remote system,. The authorization is generated by the remote system performing the following steps:

i) generating additional message attributes;

ii) generating authenticated attributes, the authenticated attributes comprising the additional message attributes and the digest;

iii) generating a digital signature of the authenticated attributes;

iv) generating a dummy data string;

v) generating a dummy authorization message with the predetermined data structure, the dummy authorization message including:

a) a digest of the dummy data string;

b) a digital signature of the digest of the dummy data string,

c) a digital certificate corresponding to the digital signature;

vi) generating the authorization message from the dummy authorization response message by making the following replacements within the dummy authorization message:

a) replacing the digest of the dummy data string with the digest of the electronic fund transfer disbursement file as provided by the server; and

b) replacing the digital signature of the digest of the dummy data string with the digital signature of the digest of the electronic fund transfer

disbursement file; and

D. the server further combining the electronic fund transfer disbursement file with the authorization message to create the electronic fund transfer submission; and

E. transferring the electronic fund transfer submission to the payments processor.

Like claim 1, with respect to claim 1, at least steps v) and vi) are not taught or suggested by Linehan, Candelore et al., nor the other art of record.

Claims 5, 6, 8, 11, and 12.

Each of claims 5, 6, 8, 11 and 12 depend from one of independent claims 1 or 7 and therefore can be distinguished over Linehan, Candelore et al. and the other art of record for the same reasons. Further, the additional elements and or steps recited in such claims further distinguish such claims over Linehan, Candelore et al. and the other art of record.

II. CONCLUSION

Accordingly, claims 1, 5-8, and 11-12 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should a petition for an extension of time be necessary for the timely reply to the outstanding Office Action (or if such a petition has been made and an additional extension is necessary), petition is hereby made and the Commissioner is authorized to charge any fees (including additional claim fees) to Deposit Account No. 501825.

Serial No.: 10/776,407

Respectfully submitted,

Timothy P. O'Hagan
Reg. No. 39,319

DATE: 11-23-05

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300